

PATENT
09/801,614

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: : Group Art Unit: 2143
: Examiner J. B. Dennison
Gerald F. McBrearty et al. : Confirmation No. 5324
Serial No: 09/801,614 :
Filed: 03/08/2001 :
Title: PROTECTING CONTENTS :
OF COMPUTER DATA FILES FROM :
SUSPECTED INTRUDERS BY :
PROGRAMMED FILE DESTRUCTION : Customer No. 32,329
Date: 05/27/08 :

BRIEF ON APPEAL

Commissioner for Patents
P.O.Box 1450
Alexandria, VA 22313-1450

Sir:

This is an Appeal from the Final Rejection of Claims 1, 4, 5, 7, 10, 13, 14, 17, 20, and 31-35 of this Application dated December 26, 2007. Section VIII. Appendix containing a copy of each of the Claims is attached.

Fee Waiver Request

It is respectfully requested that the fee for this Brief on Appeal be waived as the Appellant has already paid an Appeal Brief fee herein, which resulted in a Board Decision Reversing the Rejection, after which the Examiner has issued a new rejection which resumed the prosecution herein. Should there be any charge herein, please charge Deposit Account 09-0447.

I. Real Party in Interest

The real party in interest is International Business Machines Corporation, the assignee of the present Application.

II. Related Appeals and Interferences

Cross-referenced Application, SN. 09/801,612, G. F. McBrearty et al. filed on March 08, 2001, concurrently with the present Application is on Appeal before the Board of Appeals.

III. Status of Claims

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

There are 14 claims in this Application.

B. STATUS OF ALL THE CLAIMS

1. Claims cancelled: 2, 3, 6, 8, 9, 11, 12, 15, 16, 18, 19, and 21-30.

2. Claims withdrawn from consideration but not cancelled: None.

3. Claims pending: 1, 4, 5, 7, 10, 13, 14, 17, 20, and 31-35.

4. Claims allowed: None.

5. Claims rejected: 1, 4, 5, 7, 10, 13, 14, 17, 20, and 31-35.

C. CLAIMS ON APPEAL

Claims on appeal: 1, 4, 5, 7, 10, 13, 14, 17, 20, and 31-35.

IV Status of Amendments

No amendments have been filed after Final Rejection.

V. Summary of Claimed Subject Matter

Claim 1 is annotated with respect to the Specification and Drawings as follows.

1. In a data processing operation having stored data in a plurality of data files, a system for protecting said data files from unauthorized users comprising:

means for storing for each of said plurality of data files, a backup file inaccessible to user requests (specification, page 4, lines 3-5, file systems 70 and 71, Fig. 1 protected by firewall 66);

means for receiving user requests for access to data files (Specification, p. 10 lines 22-27 referring to Fig 4, steps 88-90);

means for determining, without accessing any of said backup files, whether said requests are unauthorized intrusions into said requested data files (Specification p.10 line 25 through page 11, line 34, referring to steps 93-97, Fig 4; there is no accessing of the backup files - only an authorization check);

means responsive to an initial determination that a request is unauthorized for destroying the requested data files (Specification, page 11, lines 7-12, referring to steps 97 and 98, Fig. 4 of the drawings); and

means for reloading a backup file for each destroyed file (page 12, lines 1-6, with reference to Fig. 4, step 99).

Claim 5 is annotated with respect to the Specification and Drawings as follows.

5. In a communication network (network of Fig. 1, described on page 6, lines 1-12) with access to a plurality of network sites (Web sites 62-64, lines 2-5, page 6) each having stored data in a plurality of data files (data file systems 70 and 71, described on page 6, lines 9-10) accessible in response to requests from users at other sites in the network (user stations 57, described on page 6, lines 12-15), a system for protecting said network site data files from unauthorized users comprising:

means for storing for each of said plurality of data files at said network site, a backup file inaccessible to user requests (specification, page 4, lines 3-5, file systems 70 and 71, Fig. 1 protected by firewall 66);

means associated with a network site for receiving user requests for access to data files (Specification, p. 10 lines 22-27 referring to Fig 4, steps 88-90);

means at said network site for determining, without accessing any of said backup files, whether said user requests are unauthorized intrusions into said requested data files (Specification p.10 line 25 through page 11, line 34, referring to steps 93-97, Fig 4; there is no accessing of the backup files - only an authorization check);

means at said network site responsive to an initial determination that a request is unauthorized for destroying the requested data files (Specification, page 11, lines 7-12, referring to steps 97 and 98, Fig. 4 of the drawings); and

means for reloading a backup file for each destroyed file (page 12, lines 1-6, referring to Fig. 4, step 99).

Claim 7 is annotated with respect to the Specification and Drawings as follows.

7. In a World Wide Web communication network (network of Fig. 1, described on page 6, lines 1-12) with access to a plurality of open Web sites (Web sites 62-64, lines 2-5, page 6) each having stored data in a plurality of data files (data file systems 70 and 71, described on page 6, lines 9-10) accessible in response to requests from users at stations throughout the Web (user stations 57, described on page 6, lines 12-15), a system for protecting said open Web site data files from unauthorized users comprising:

means for storing for each of said plurality of data files at said open Web site, a backup file inaccessible to user requests (specification, page 4, lines 3-5, file systems 70 and 71, Fig. 1 protected by firewall 66);

means associated with an open Web site for receiving user requests for access to data files (Specification, p. 10 lines 22-27 referring to Fig 4, steps 88-90);

means at said open Web site for determining, without accessing any of said backup files, whether said user requests are unauthorized intrusions into said requested data files (Specification p.10 line 25 through page 11, line 34, referring to steps 93-97, Fig 4; there is no accessing of the backup files - only an authorization check);

means at said open Web site responsive to an initial determination that a request is unauthorized for destroying the requested data files (Specification, page 11, lines 7-12, referring to steps 97 and 98, Fig. 4 of the drawings);
and

means for reloading a backup file for each destroyed file (page 12, lines 1-6, referring to Fig. 4, step 99).

Claim 10 is annotated with respect to the Specification and Drawings as follows.

10. In a data processing operation having stored data in a plurality of data files, a method for protecting said data files from unauthorized users comprising:

storing for each of said plurality of data files, a backup file inaccessible to user requests (Specification, page 4, lines 3-5, file systems 70 and 71, Fig. 1 protected by firewall 66);

receiving user requests for access to data files (Specification, p. 10 lines 22-27 referring to Fig 4, steps 88-90);

determining, without accessing any of said backup files, whether said requests are unauthorized intrusions into said requested data files (Specification p.10 line 25 through page 11, line 34, referring to steps 93-97, Fig 4; there is no accessing of the backup files - only an authorization check);

destroying the requested data files responsive to an initial determination that a request is unauthorized (Specification, page 11, lines 7-12, referring to steps 97 and 98, Fig. 4 of the drawings); and

reloading a backup file for each destroyed file (page 12, lines 1-6, with reference to Fig. 4, step 99).

Claim 14 is annotated with respect to the Specification and Drawings as follows.

14. In a communication network (network of Fig. 1, described on page 6, lines 1-12) with access to a plurality of network sites (Web sites 62-64, lines 2-5, page 6) each having stored data in a plurality of data files (data file systems 70 and 71, described on page 6, lines 9-10) accessible in response to requests from users at other sites in the network (user stations 57, described on page 6, lines 12-15), a method for protecting said network site data files from unauthorized users comprising:

storing for each of said plurality of data files at said network site, a backup file inaccessible to user requests (specification, page 4, lines 3-5, file systems 70 and 71, Fig. 1 protected by firewall 66);

receiving user requests for access to data files at a network site (Specification, p. 10 lines 22-27 referring to Fig 4, steps 88-90);

determining at said network site, without accessing any of said backup files, whether said user requests are unauthorized intrusions into said requested data files (Specification p.10 line 25 through page 11, line 34, referring to steps 93-97, Fig 4; there is no accessing of the backup files - only an authorization check);

destroying the requested data files responsive to an initial determination that a request is unauthorized (Specification, page 11, lines 7-12, referring to steps 97 and 98, Fig. 4 of the drawings); and

reloading a backup file for each destroyed file (page 12, lines 1-6, referring to Fig. 4, step 99).

Claim 17 is annotated with respect to the Specification and Drawings as follows.

17. In a World Wide Web communication network (network of Fig. 1, described on page 6, lines 1-12) with access to a plurality of open Web sites (Web sites 62-64, lines 2-5, page 6) each having stored data in a plurality of data files (data file systems 70 and 71, described on page 6, lines 9-10) accessible in response to requests from users at stations throughout the Web (user stations 57, described on page 6, lines 12-15), a method for protecting said open Web site data files from unauthorized users comprising:

storing for each of said plurality of data files at said open Web site, a backup file inaccessible to user requests (Specification, page 4, lines 3-5, file systems 70 and 71, Fig. 1 protected by firewall 66);

receiving user requests for access to data files at said open Web site (Specification, p. 10 lines 22-27 referring to Fig 4, steps 88-90);

determining, without accessing any of said backup files, whether said user requests are unauthorized intrusions into said requested data files at said open Web site (Specification p. 10 line 25 through page 11, line 34, referring to steps 93-97, Fig 4; there is no accessing of the backup files - only an authorization check);

destroying the requested data files at said open Web site responsive to an initial determination that a request is unauthorized (Specification, page 11, lines 7-12, referring to steps 97 and 98, Fig. 4 of the drawings); and

reloading a backup file for each destroyed file (page 12, lines 1-6, referring to Fig. 4, step 99).

Claim 31 is annotated with respect to the Specification and Drawings as follows.

31. A computer readable medium having stored thereon a computer readable program (page 8 lines 14-25, with reference to Fig. 2, describes the storage of the program 40 on a computer readable medium RAM 14) for protecting data stored in a plurality of data files from unauthorized users, wherein the computer readable program when executed on a computer (With respect to Fig. 3, page 9, lines 16-20 introduces the computer program which when executed, Fig. 4, page 10, lines 12-15, and subsequently performs the steps which follow) causes the computer to:

store for each of said plurality of data files, a backup file inaccessible to user requests (Specification, page 4, lines 3-5, file systems 70 and 71, Fig. 1 protected by firewall 66);

receive user requests for access to data files (Fig. 4, step 88, page 10, lines 23-25);

determine, without accessing any of said backup files, whether said requests are unauthorized intrusions into said requested data files (Specification p. 10 line 25 through page 11, line 34, referring to steps 93-97, Fig 4; there is no accessing of the backup files - only an authorization check);

destroy the requested data files responsive to an initial determination that a request is unauthorized (Specification, page 11, lines 7-12, referring to steps 97 and 98, Fig. 4 of the drawings); and

reload a backup file for each destroyed file (page 12, lines 1-6, with reference to Fig. 4, step 99).

Claim 33 is annotated with respect to the Specification and Drawings as follows.

33. A computer readable medium having stored thereon a computer readable program (page 8 lines 14-25, with reference to Fig. 2, describes the storage of the program 40 on a computer readable medium RAM 14) for protecting, from unauthorized users, data stored in a plurality of data files at network sites accessible in response to requests from users at other sites in the network, wherein the computer readable program when executed on a computer causes the computer (With respect to Fig. 3, page 9, lines 16-20 introduces the computer program which when executed, Fig. 4, page 10, lines 12-15, and subsequently performs the steps which follow) to:

store for each of said plurality of data files at said network sites, a backup file inaccessible to user requests (specification, page 4, lines 3-5, file systems 70 and 71, Fig. 1 protected by firewall 66);

receive user requests for access to data files at a network site (Specification, p. 10 lines 22-27 referring to Fig 4, steps 88-90);

determine at said network site, without accessing any of said backup files, whether said user requests are unauthorized intrusions into said requested data files (Specification p.10 line 25 through page 11, line 34, referring to steps 93-97, Fig 4; there is no accessing of the backup files - only an authorization check);

destroy the requested data files responsive to an initial determination that a request is unauthorized (Specification, page 11, lines 7-12, referring to steps 97 and 98, Fig. 4 of the drawings); and

reload a backup file for each destroyed file (page 12, lines 1-6, with reference to Fig. 4, step 99).

Dependent Claim 4 (argued separately) is annotated as follows with respect to the Specification and Drawings.

4. The data processing operation system of claim 1 wherein said means for determining whether said user requests are unauthorized intrusions include:

means for determining whether a user access identification code has been denied (Specification: page 4, lines 13-25); and

means for determining whether the user has copied the requested files (Specification: page 4, lines 13-25).

Dependent Claim 13 (argued separately) is annotated as follows with respect to the Specification and Drawings.

13. The data processing method of claim 10 wherein said step of determining whether said user requests are unauthorized intrusions includes:

determining whether a user access identification code has been denied (Specification: page 4, lines 13-25); and

determining whether the user has copied the requested files (Specification: page 4, lines 13-25).

Dependent Claim 20 (argued separately) is annotated as follows with respect to the Specification and Drawings.

20. The World Wide Web communication network method of claim 17 wherein said step of determining whether said user requests are unauthorized intrusions includes:

determining whether a user access identification code has been denied (Specification: page 4, lines 13-25); and

determining whether the user has copied the requested files (Specification: page 4, lines 13-25).

Dependent Claim 32 (argued separately) is annotated as follows with respect to the Specification and Drawings.

32. The computer readable medium of claim 31, wherein in determining whether said user requests are unauthorized intrusions, the computer readable program causes the computer to:

determine whether a user access identification code has been denied (Specification: page 4, lines 13-25); and

determine whether the user has copied the requested files (Specification: page 4, lines 13-25).

Dependent Claim 34 (argued separately) is annotated as follows with respect to the Specification and Drawings.

34. The computer readable medium of claim 33, wherein the network is the World wide Web and said network sites are Web sites (Fig 1 shows a Web 50 network, described at page 6, lines 2-5).

VI. Grounds of Rejection to be Reviewed on Appeal

A. Claims 1, 5, 7, 10, 14, 17, 31, and 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Winburn (US2002/0069363).

B. Claims 4, 13, 20, 32, 34, and 35 are rejected under 35 U.S.C. 103(a) as unpatentable over Winburn (US2002/0069363) in view of Moran (US6,647,400) and Koelle et al. (US7,150,045).

VII. Argument

Claims 1, 5, 7, 10, 14, 17, 31, and 33 are not anticipated by, and thus patentable under 35 U.S.C. 102(e) over Winburn (US2002/0069363).

In order for a reference to anticipate a claimed invention under 35 USC 102, the reference must disclose every element of the claimed invention without modification.

All of the claims now recite the element:

"....determining, without accessing any of said backup files, whether said user requests are unauthorized intrusions into said requested data files;"

Winburn fails to teach the element of determining, without accessing any of said backup files, whether said user requests are unauthorized intrusions into said requested data files. Accordingly, Winburn fails to satisfy the requirements of an anticipatory reference under 35 U.S.C. 102(e). Winburn must access and compare his backup files or elements of his backup files to the respective current or active files or corresponding elements in his current files in order to authenticate whether the contents of the current files have compromised. Thus, Winburn fails to teach the element of determining, without accessing any

of said backup files, whether said user requests are unauthorized intrusions into said requested data files.

In this connection, Appellants submit that they did not intend to argue that Winburn just compares the total content of his current i.e. active files to the total content of his backup files in determining whether there has been an unauthorized intrusion. However, Winburn does teach the comparison of elements (identifiers) derived from the contents of his backup files with elements (identifiers) derived from the content of his current or active files to determine whether there has been an unauthorized intrusion. On this point, Appellants submit that in order to create the identifiers from the content of his backup files, Winburn must access such backup files. Thus, Winburn fails to disclose:

"....determining, without accessing any of said backup files, whether said user requests are unauthorized intrusions into said requested data files;"

In response to Appellants' arguments, Examiner has referred to Section 0008, commencing on page 1 of the Winburn publication. Appellants submit that this section teaches the identifier which Winburn uses for comparison is produced using one or more attributes of the authorized protected data file i.e. the backup file. Appellants submit that in order to produce the identifier from his backup file, Winburn must access his backup file. Thus, the element: "determining, without accessing any of said backup files, whether said user requests are unauthorized intrusions" is not taught by Winburn.

Accordingly, Winburn fails as an anticipatory reference in the rejection of claims 1, 5, 7, 10, 14, 17, 31, and 33 under 35 U.S.C. 102(e) because it does not disclose every

element of the claimed invention without modification.

Dependent Claims 4, 13, 20, 32, 34, and 35 are Unobvious under 35 U.S.C. 103(a) and Patentable over Winburn (US2002/0069363) in view of Moran (US6,647,400) and Koelle et al. (US7,150,045)

With respect to dependent claims 4, 13, 20, 32, and 35, these claims cover a further embodiment of the above described general invention wherein an unauthorized intrusion is determined by determining whether a user access identification has been denied and whether the user (intruder) has already copied the requested files. These claims are submitted to be patentable over Winburn for all of the reasons set forth hereinabove for the patentability of independent claims from which these claims respectively depend. In addition, these dependent claims cover a combination of events which would indicate an immediate unauthorized intrusion. Even if the modifying Moran and Koelle patents could arguably be said to suggest these events of previous denial of ID or previous copying defined in these dependent claims, these claims are submitted to be patentable for the reasons set forth for the patentability of the independent claims.

Likewise, with respect to dependent claim 34, if it be conceded that Web network transactions are known, dependent claim 34 is submitted to be patentable for the reasons set forth hereinabove for the patentability of independent claim 33 from which claim 34 depends.

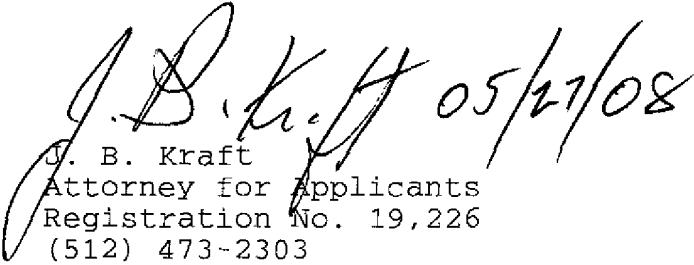
PATENT
09/801,614

Conclusion

In view of the foregoing, claims 1, 4, 5, 7, 10, 13, 14, 17, 20, and 31-35 are submitted to be patentable.

Accordingly, the Board of Appeals is respectfully requested to reverse the final rejection and find claims 1, 4, 5, 7, 10, 13, 14, 17, 20, and 31-35 in condition for allowance.

Respectfully submitted,

 05/27/08
J. B. Kraft
Attorney for Applicants
Registration No. 19,226
(512) 473-2303

ALL CORRESPONDENCE SHOULD BE DIRECTED TO:

Herman Rodriguez
IPLaw Dept.
IBM Corporation
11400 Burnet Road
Austin, Texas 78758

VIII. Claims Appendix

1 1. In a data processing operation having stored data in a
2 plurality of data files, a system for protecting said data
3 files from unauthorized users comprising:

4 means for storing for each of said plurality of data
5 files, a backup file inaccessible to user requests;

6 means for receiving user requests for access to data
7 files;

8 means for determining, without accessing any of said
9 backup files, whether said requests are unauthorized
10 intrusions into said requested data files;

11 means responsive to an initial determination that a
12 request is unauthorized for destroying the requested data
13 files; and

14 means for reloading a backup file for each destroyed
15 file.

1 4. The data processing operation system of claim 1 wherein
2 said means for determining whether said user requests are
3 unauthorized intrusions include:

4 means for determining whether a user access identifica-
5 tion code has been denied; and

6 means for determining whether the user has copied the
7 requested files.

1 5. In a communication network with access to a plurality of
2 network sites each having stored data in a plurality of data
3 files accessible in response to requests from users at other
4 sites in the network, a system for protecting said network
5 site data files from unauthorized users comprising:
6 means for storing for each of said plurality of data
7 files at said network site, a backup file inaccessible to
8 user requests;
9 means associated with a network site for
10 receiving user requests for access to data files;
11 means at said network site for determining, without
12 accessing any of said backup files, whether said user
13 requests are unauthorized intrusions into said requested
14 data files;
15 means at said network site responsive to an initial
16 determination that a request is unauthorized for destroying
17 the requested data files; and
18 means for reloading a backup file for each destroyed
19 file.

1 7. In a World Wide Web communication network with access to
2 a plurality of open Web sites each having stored data in a
3 plurality of data files accessible in response to requests
4 from users at stations throughout the Web, a system for
5 protecting said open Web site data files from unauthorized
6 users comprising:
7 means for storing for each of said plurality of data
8 files at said open Web site, a backup file inaccessible to
9 user requests;
10 means associated with an open Web site for
11 receiving user requests for access to data files;
12 means at said open Web site for determining, without
13 accessing any of said backup files, whether said user
14 requests are unauthorized intrusions into said requested
15 data files;
16 means at said open Web site responsive to an initial
17 determination that a request is unauthorized for destroying
18 the requested data files; and
19 means for reloading a backup file for each destroyed
20 file.

1 10. In a data processing operation having stored data in a
2 plurality of data files, a method for protecting said data
3 files from unauthorized users comprising:
4 storing for each of said plurality of data files, a
5 backup file inaccessible to user requests;
6 receiving user requests for access to data files;
7 determining, without accessing any of said backup
8 files, whether said requests are unauthorized intrusions
9 into said requested data files;
10 destroying the requested data files responsive to an
11 initial determination that a request is unauthorized; and
12 reloading a backup file for each destroyed file.

1 13. The data processing method of claim 10 wherein said
2 step of determining whether said user requests are unautho-
3 rized intrusions includes:

4 determining whether a user access identification code
5 has been denied; and

6 determining whether the user has copied the requested
7 files.

1 14. In a communication network with access to a plurality
2 of network sites each having stored data in a plurality of
3 data files accessible in response to requests from users at
4 other sites in the network, a method for protecting said
5 network site data files from
6 unauthorized users comprising:

7 storing for each of said plurality of data files at
8 said network site, a backup file inaccessible to user re-
9 quests;

10 receiving user requests for access to data files at a
11 network site;

12 determining at said network site, without accessing any
13 of said backup files, whether said user requests are
14 unauthorized intrusions into said requested data files;

15 destroying the requested data files responsive to an
16 initial determination that a request is unauthorized; and

17 reloading a backup file for each destroyed file.

1 17. In a World Wide Web communication network with access
2 to a plurality of open Web sites each having stored data in
3 a plurality of data files accessible in response to requests
4 from users at stations throughout the Web, a method for
5 protecting said open Web site data files from unauthorized
6 users comprising:
7 storing for each of said plurality of data files at
8 said open Web site, a backup file inaccessible to user
9 requests;
10 receiving user requests for access to data files at
11 said open Web site;
12 determining, without accessing any of said backup
13 files, whether said user requests are unauthorized
14 intrusions into said requested data files at said open Web
15 site;
16 destroying the requested data files at said open Web
17 site responsive to an initial determination that a request
18 is unauthorized; and
19 reloading a backup file for each destroyed file.

1 20. The World Wide Web communication network method of
2 claim 17 wherein said step of determining whether said user
3 requests are unauthorized intrusions includes:
4 determining whether a user access identification code
5 has been denied; and
6 determining whether the user has copied the requested
7 files.

1 31. A computer readable medium having stored thereon a
2 computer readable program for protecting data stored in a
3 plurality of data files from unauthorized users, wherein the
4 computer readable program when executed on a computer causes
5 the computer to:
6 store for each of said plurality of data files, a
7 backup file inaccessible to user requests;
8 receive user requests for access to data files;
9 determine, without accessing any of said backup files,
10 whether said requests are unauthorized intrusions into said
11 requested data files;
12 destroy the requested data files responsive to an
13 initial determination that a request is unauthorized; and
14 reload a backup file for each destroyed file.

1 32. The computer readable medium of claim 31, wherein in
2 determining whether said user requests are unauthorized
3 intrusions, the computer readable program causes the
4 computer to:
5 determine whether a user access identification code has
6 been denied; and
7 determine whether the user has copied the requested
8 files.

1 33. A computer readable medium having stored thereon a
2 computer readable program for protecting, from unauthorized
3 users, data stored in a plurality of data files at network
4 sites accessible in response to requests from users at other
5 sites in the network, wherein the computer readable program
6 when executed on a computer causes the computer to:
7 store for each of said plurality of data files at said
8 network sites, a backup file inaccessible to user requests;
9 receive user requests for access to data files at a
10 network site;
11 determine at said network site, without accessing any
12 of said backup files, whether said user requests are
13 unauthorized intrusions into said requested data files;
14 destroy the requested data files responsive to an
15 initial determination that a request is unauthorized; and
16 reload a backup file for each destroyed file.

1 34. The computer readable medium of claim 33, wherein the
2 network is the World wide Web and said network sites are Web
3 sites.

1 35. The computer readable medium of claim 34, wherein in
2 determining whether said user requests are unauthorized
3 intrusions, the computer readable program causes the
4 computer to:
5 determine whether a user access identification code has
6 been denied; and
7 determine whether a user has copied the requested
8 files.

PATENT
09/801,614

IX. Evidence Appendix

There is no evidence presented.

X. Related Proceedings Appendix

There has been no decision as yet in the Appeal before the Board in related Cross-referenced Application, SN. 09/801,612, G. F. McBrearty et al. filed on March 08, 2001, concurrently with the present Application as mentioned hereinabove in Section II.